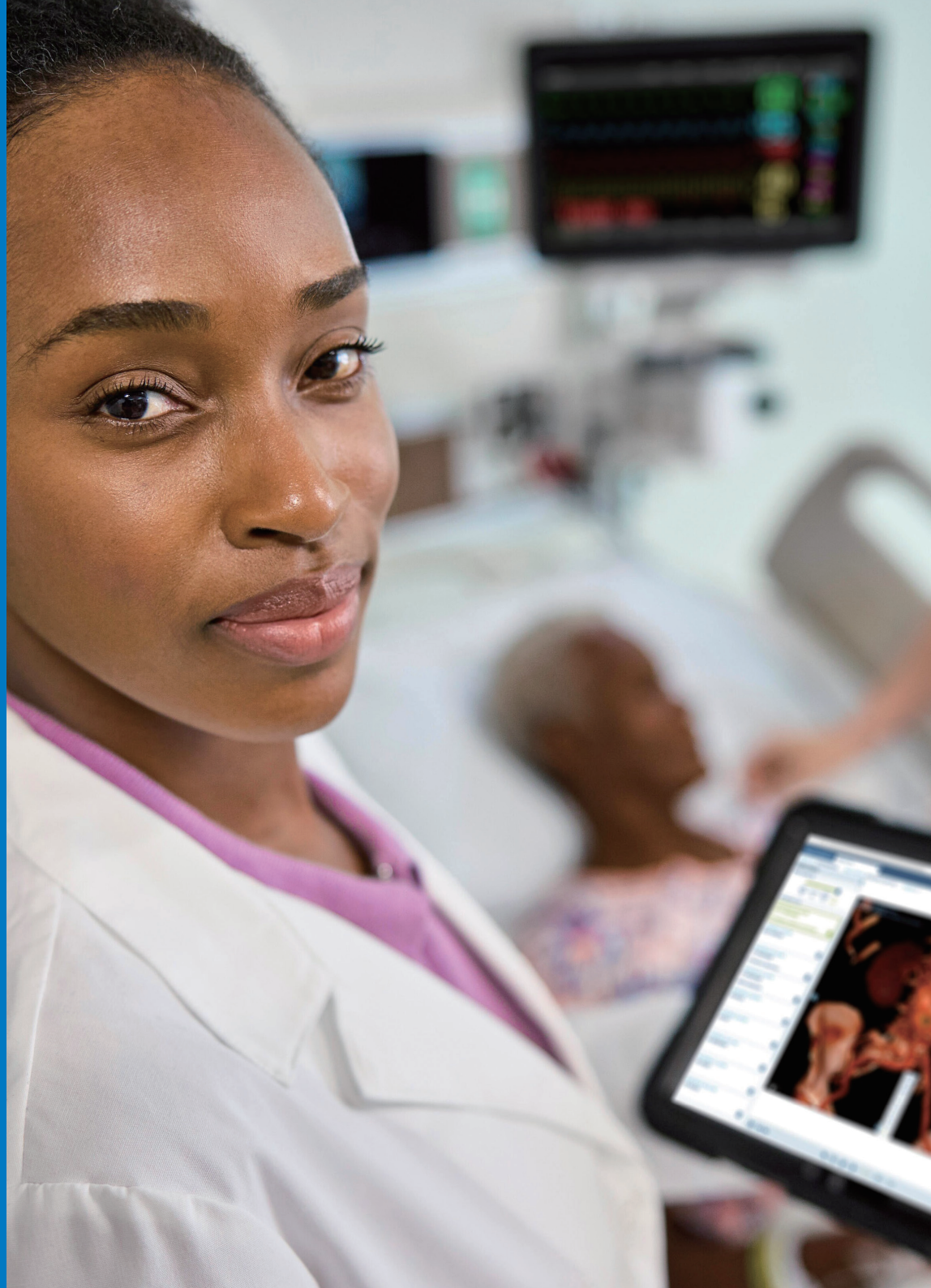
PHILIPS

Cybersecurity Position paper, June 2025

お客様のセキュリティ課題へのフィリップスの積極的な取り組み



目次

ヘルスケアのデジタル化 – 機会と脅威

今日のヘルスケアシステムは、高齢化の進行と慢性疾患の増加という課題に直面しています。また、医療業界は、適正な価格のケアモデルの開発に取り組んでいます。機器や健康アプリ、プラットフォームによって可能になるコネクテッドヘルスケアは、ヘルスケアを変革し、よりよい健康とよりよいケアを低コストで実現する可能性を秘めています。

ネットワークを介して接続されたデジタルデバイスの普及により、ユーザーは、ケアの成果を向上させることに活用できる膨大なデータフローを共有、検索、ナビゲート、管理、比較、分析できるようになりました。

このデジタル「エコシステム」は、ヘルスケア業界において、個人用のヘルスケア指向のスマートデバイスのポートフォリオを拡大して、システムを刷新し、サービスの効率を向上させるのに役立っています。

例えば、電子医療記録の分析や、画像診断装置、モニター、携帯型の個人用機器で収集した診断情報の分析により、医療従事者の意思決定能力が向上しただけでなく、人々が自身の健康を管理するうえでより重要な役割を果たすようになりました。

その一方で、データの量と種類の急激な増加は、サイバー犯罪につながる脆弱性の増加をもたらしています。世界の医療機関の90%以上が、過去数年間に少なくとも1件のセキュリティ侵害を報告しています。[1] さらに、医療業界におけるデータ侵害は、他の業界に比べて経済的な損害が大きく、平均977万米ドルにもなっています。[2]

医療記録に含まれる個人情報は、個人情報の盗用や保険金詐欺など、さまざまな悪意のある目的に使用されるほど、利用価値が高い情報となっています。

医療機関への脅威には、ウイルス、ワーム、ハッカーの侵入による悪意のあるサイバー攻撃が含まれます。攻撃者は、屋根裏部屋のハッカーから組織犯罪、さらには国家まで多岐にわたります。

1 Palatty, 80+ Healthcare Data Breach Statistics 2024, Astra, February 6, 2025.
2 IBM, Cost of a Data Breach Report 2024.

ランサムウェア攻撃の世界的な急増は、最大規模かつ最先端の組織であっても、攻撃による混乱に対して脆弱になり得ることを示しています。このような事例において、一部の病院では別の医療機関へ患者の転院を余儀なくされました。

新型コロナウイルスの大流行期に急増したリモートワークと電子商取引は、新たなサイバーセキュリティの課題を数多くもたらしました。

「セキュリティは最優先事項です」

Shez Partovi
Chief Innovation & Strategy Officer, Royal Philips

サイバーセキュリティにおけるフィリップスの姿勢

フィリップスは、消費者と医療従事者がより容易に連携し、より適切な情報に基づいた意思決定を行えるように支援する技術を提供しています。このような技術革新において影響力があって期待されるもののいくつかは、大規模な研究グループやビッグデータセットに関する研究に関係しています。

そのような情報の安全性を確保することは、フィリップスにとって重要な優先事項です。これは、当社の戦略的な立場と競争力が、データおよびデジタル技術、消費者の信用に大きく依存するためです。当社のセキュリティ部門からの推奨事項、監査結果やその他の適切な情報提供を基に、四半期ごとの報告はセキュリティ分野の優先事項とリスク許容度を決定しています。

お客様や消費者の懸念や、現代の相互接続されたデジタル「エコシステム」においてセキュリティが果たす重大な役割を踏まえ、フィリップスは、製品、ビジネス（エンタープライズ情報）、および個人（患者）情報の安全性を確保する包括的なセキュリティ戦略の展開に取り組んでいます。

当社のセキュリティ戦略（「セキュアバイデザイン（Secure by Design）」と呼ばれる）は、人、プロセスおよび技術を包含しています。このアプローチの目的は、重要なデータとそのデータを格納するシステムの機密性、完全性、可用性を確保することです。

「セキュアバイデザイン」は、システムとそのコンポーネントの設計時からセキュリティが最優先に考慮される統合的なアプローチです。このようにして、健康情報と医療機器はライフサイクル全体にわたって保護され、セキュリティの確保を図ります。

安全性と品質と同様に、セキュリティは、フィリップスブランドの価値を守る前提条件です。お客様と消費者には、当社の製品とサービスのセキュリティ、安全性、品質についての高い評価をいただくことが重要です。そのため、これからも当社は、コネクテッドヘルスケアテクノロジーのメリットを積極的に紹介しつつ、お客様が快適に使用できるセキュアなシステムへの投資を続けていきます。

「フィリップスは、医療従事者がセキュアな環境で患者のケアに集中できるように支援します。複雑で急拡大するエコシステムにおいて、パートナーシップこそがシームレスでセキュアなサービスを提供する鍵となります」

Gal Gnainsky
Chief Security Officer, Royal Philips

透明性、コンプライアンス、そしてその先へ

フィリップスは、厳しく規制された医療機器業界でセキュリティ対策を実施しています。アメリカ食品医薬品局（FDA）や欧州医療機器規則（EU MDR）などの規制当局およびポリシーによって、対象となるすべてのフィリップスの製品とサービスにおいて、安全性、セキュリティ、有効性、品質および性能の高い基準を満たすことを保証するために、ハードウェアおよびソフトウェアのリリースや変更は、厳格な検証および妥当性確認の方法に従うことが要求されています。

フィリップスは、脆弱性の報告および対応に関してオープンかつ透明性を確保することに努め、強固な協調的脆弱性開示プロセスを開発しています。

当社の戦略は、新たに発生するセキュリティの脆弱性と潜在的な外部の脅威を常に把握し、規制当局や業界のパートナー企業、医療従事者などと協力して、セキュリティホールを塞ぎ、安全対策を実施することです。

フィリップスは、セキュリティやプライバシーに重点を置く主要な業界団体に積極的に参加し、当社の取り組みをさらに整えています。当社は、適切かつ必要なお客様向けのセキュリティ要件が業界の標準やガイドライン、イニシアティブに含まれるよう、努めています。

当社は、医療業界が直面しているサイバーセキュリティリスクの緊急性と複雑さを示す報告書を発行した、米国保健福祉省（HHS）のセキュリティタスクフォースの創設メンバーでした。この取り組みは、業界のワーキンググループに影響を与え続けています。当社は、国際標準化機構（ISO）や国際電気標準会議（IEC）を含む複数の標準化団体を通じて、医療分野のセキュリティ標準の策定に積極的に参画しています。

「お客様との連携と透明性を維持することで、当社は、患者の安全性向上を目的として、継続的な製品とサービスのセキュリティ向上に取り組んでいます。」

Dirk de Wit
Head of Product Security, Royal Philips

製品セキュリティ

フィリップスは、当社製品に対するサイバーセキュリティの脅威のリスクが高まっていることを深刻に受け止めています。フィリップスのセキュリティファーストのアプローチによって、当社のソリューションとサービスに関わる患者のリスクを抑えるために、プロセスとシステムを改善する取り組みが継続できています。

フィリップスは、さまざまな業界で起きている巧妙なサイバー攻撃が、特に医療分野で増加していることを強く認識しています。院内ネットワーク、臨床データベース、医療機器、およびパーソナルヘルスモニタリングシステムがより統合されるにしたがって、サイバーセキュリティの脆弱性による潜在的影響は増大し続けています。

フィリップスは、効果的なサイバーセキュリティがもはや「ボックス」や個々の製品の保護ではなく、どこで、どのように機器が使用されるかを考慮した体系的なアプローチが必要であることをいち早く認識していました。そのため当社は、業界全体で協調的脆弱性開示（Coordinated Vulnerability Disclosure：CVD）が採用される3年前に、協調的脆弱性管理プロセスを導入しました。さらに、フィリップスは、セキュリティテストにおいて、業界でも先駆けて、2019年にUL2900認証を取得した医療機器製造業者になりました。

フィリップスの製品セキュリティ部門は、フィリップスエクセレンスフレームワークの一部である製品セキュリティフレームワークを通じて、すべての製品とサービスへのセキュリティの組み込みをライフサイクル全体にわたって管理しています。このセキュリティフレームワークには、製品セキュリティのリスクアセスメント、独立した脆弱性およびペネトレーション評価、専門的な製品セキュリティトレーニング、および保守・サポート契約の対象である既存の製品とサービスで特定された脆弱性に対する対応業務が含まれます。

フィリップスにおいて「セキュアバイデザイン」とは、製品の設計・開発からテスト・展開まで、セキュリティの原則を組み込んでいるエンドツーエンドの考え方です。このアプローチは、モニタリング、効率的な更新およびインシデント対応の管理に関する強固なポリシーと手順によってサポートされています。

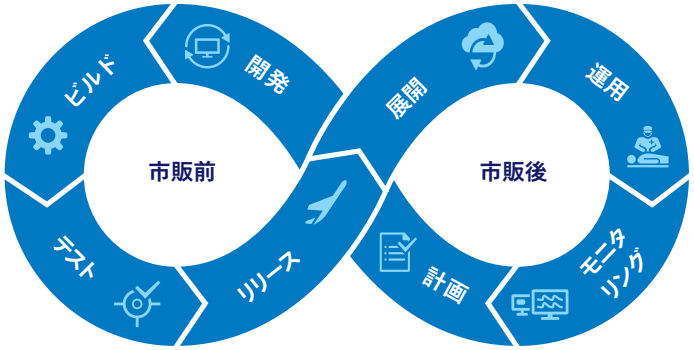
当社の製品とサービスをサイバー脅威に対して強固にするためには、リスクアセスメントへのコミットメント、およびセキュリティに基づいた製品開発の順守が必要になります。そのためには、暗号化やパッチ管理などのセキュリティを実現する技術の迅速な展開、およびこれらの継続的な改善が求められます。このような理由から、当社はお客様の要件を満たすための包括的かつ実践的なアプローチを作成、実装、および更新すべく、Product and Solutions Security Program（製品およびソリューションセキュリティプログラム）を策定しました。

フィリップスの製品セキュリティの主要な取り組み

フィリップスは、Philips Product Security Policy（フィリップス製品セキュリティポリシー）を遵守しています。このポリシーは、組織がセキュリティにおけるベストプラクティスを実践できるように、ポリシー、手順、タイムリーに文書化された対応策から構成されています。

このポリシーは、以下の当社の戦略的な組織と手順について定義しています。

- セキュリティ専門家のグローバルネットワークの維持
- 新製品の開発開始時に潜在的脅威を事前予防的に評価するための脅威モデリング作業の管理
- 当社の製品とサービスにおけるベストプラクティスの開発および展開
- セキュリティおよびプライバシーの潜在的な脅威と潜在的な脆弱性に関するリスクアセスメント作業の管理
- 特定されたセキュリティおよびプライバシーの脅威に関するインシデント対応作業の指導
- 製品とサービスに組み込まれているセキュリティのライフサイクルを通じた管理
- クラウド環境に関する最新版のセキュリティ標準に準拠するためのHealthSuiteプラットフォームのサポート
- Secure Product Development Lifecycle（セキュアな製品開発ライフサイクル）の一環として、脆弱性の継続的なモニタリングおよび修正内容の検証（当社のSecurity Center of Excellenceによってサポートされている作業）



フィリップスのSecurity Center of Excellenceは、世界中の主要なサイバーセキュリティ研究者および試験施設と情報を共有し、サイバー脅威の迅速な除去、低減や緩和を支援しています。

現行の規制要件および業界のベストプラクティスを満たすか、またはこれを上回るセキュリティ標準の実装内容には、以下が含まれます。

- 規制当局が推奨する標準に準拠し、かつIEC/TR 80001-2-2規格の基礎として使用されている、製品およびサービスの製品セキュリティ要件
- NIST SP 800-53、ISO/IEC 27000シリーズ、HITRUSTのような認定基準に準拠したサービスセキュリティ
- Manufacturer Disclosure Statement for Medical Device Security（医療機器セキュリティのための製造業者開示説明書：MDS2）などの顧客対応情報の作成
- FDA、EU MDRおよび医療機器のサイバーセキュリティに関するその他の法律や規制への対応

フィリップスのSecurity Center of Excellenceは、IEC 62304セキュリティオプションへの登録の一環として、UL Solutionsによる包括的な監査を受けました。この監査では、Philips Security Center of Excellenceの中核である製品セキュリティプロセス（セキュリティリスクマネジメントおよびリスクコントロールの手段、ソフトウェアセキュリティ検証計画、変更管理および継続的改善、センターのラボラトリー品質マネジメントシステムを含む）のレビューと検証が行われました。

脅威、脆弱性、およびセキュリティインシデントのモニタリングと対応

- オペレーティングシステム（OS）やサードパーティソフトウェアのベンダー、お客様およびセキュリティ研究者によって特定されたものを含め、新しいセキュリティの脅威、脆弱性およびセキュリティインシデントの継続的なモニタリング
- 当社の製品セキュリティインシデント対応チームによる、潜在的なセキュリティインシデントおよび脆弱性の評価と、必要に応じた対応計画の策定

マルウェア対策ソフトおよびパッチ管理

- 市販のマルウェア対策ソフトをサポートする製品は、プレインストールされたマルウェア対策ソフト、またはお客様向け文書と共に提供される場合がある。これらの文書には、製品固有のフィリップス承認済みのマルウェア対策ソフトのパラメータが詳細に記載されている。
- フィリップス製品は、Microsoft WindowsやLinuxなどのオペレーティングシステム（OS）をはじめとするサードパーティ製ソフトウェアを使用する場合がある。当社の製品エンジニアリングチームによる、これらのホットフィックス（緊急パッチ）の影響評価は、通常、新しいセキュリティ脆弱性やパッチ提供を当社が把握してから48時間以内に開始される。
- フィリップスは、プラットフォームおよび機器の陳腐化に関連する脅威から保護するサービスを含め、ライフサイクルにおけるサイバーセキュリティリスクに対処するための多様なプログラムを展開している。

特定された脆弱性の報告および対応

- 当社は、業界におけるベストプラクティスに基づくCVDの設計および実装を行っている。
- 当社のCVDポリシーは公開されており、お客様、研究者およびその他のセキュリティコミュニティの関係者との明確なコミュニケーションチャネルを設けている。
- このポリシーは、インバウンド通信のモニタリングと対応、フォローアップの管理、脆弱性通知と状況追跡の評価、およびインシデント対応／是正措置／再発防止ポリシーとの整合性を包含している。
- 当社は、共通脆弱性識別子（CVE）の発行を行うCVE Numbering Authority（CNA）である。CVEにより、ソフトウェアのセキュリティ脆弱性に対応するための業界全体での協調的な取り組みが可能となっている。

フィリップスは、長年にわたり、戦略的かつ効率的な技術開発を通じて、医療機器のセキュリティを確保することに取り組んでいます。

製品セキュリティが医療業界において重要な課題であることに変わりはありません。当社は、「2030年までに年間25億人の人々の生活を向上させる」というパーパスの一環として、対話の促進を期待しています。

エンタープライズ情報セキュリティ

フィリップスは、当社の先進技術に対するお客様からの長年にわたる支持により成長を続けています。このような技術の設計、開発、生産を支えているのは、当社内の高度な情報システムです。

フィリップスの情報セキュリティ担当部門の目的は、エンタープライズ情報システムの保護です。急増するサイバーセキュリティの脅威は、これらの技術とその内部に保存されているデータを標的にしています。そのため、当社は以下について誠実に取り組んでいます。

- **お客様の信頼:** フィリップスブランドを、安全性、品質、セキュリティの代名詞となるよう強化する。
- **成長力:** 企業の長期的な競争力を確保するために、機密情報の損失の防止を図る。
- **財務業績:** 顧客流出や売上・利益の損失を含む財務的な悪影響を未然に防止し、企業資産の保護に取り組む。
- **運用の安定性:** 運用に不可欠なインフラの劣化や障害を防止することで、継続的な運用を目指す。
- **規制の遵守:** フィリップスは、業界のベストプラクティスおよび最新の規制要件（例：NIS2, CRA, FDA, NMPA, ISO）に基づいて評価し、重要なセキュリティ対策を継続的に改善する（エンドポイントの強化、電子メールのセキュリティおよびネットワークセキュリティの強化、脆弱性への対応を含むグローバルな脆弱性スキャンの実施など）。

情報セキュリティの課題は、技術のみでは解決できません。包括的な情報セキュリティでは、人、プロセス、技術という3つの領域に焦点を当てる必要があります。当社の情報セキュリティ部門は、以下を促進するために、これら3つの領域の対策を実施しています。

- **機密性:** アクセス権限を有する者のみがデータを取得できる。
- **完全性:** 情報は、検知されずに改ざんされることは認められない。
- **可用性:** 必要なときに情報にアクセスできる。

フィリップスは、エンタープライズ情報システムのセキュリティを確保し、進化する脅威の状況に対応し続けています。当社の情報セキュリティ部門は、経験豊富なサイバーセキュリティの人材の確保、サイバーセキュリティツールや機能の強化のほか、当社が行うあらゆることにおいて、セキュリティのベストプラクティスを統合することに投資を集中することに責任をもって取り組んでいます。

情報セキュリティにおける人、プロセス、技術への注力

人
従業員の行動面に焦点を当て、従業員のセキュリティ意識を向上させ、結果としてセキュリティ文化を発展させます。

プロセス
当社の業務プロセスに焦点を当て、セキュリティリスクを評価し、リスクを軽減するための適切な対策をプロセスに組み込んでいます。

技術
当社技術の全体像の把握とモニタリングに焦点を当て、セキュリティリスクに対する態勢を強化するために、技術的改善を図ります。

社会的な観点で、サイバーセキュリティのレジリエンス（耐性）が重要な懸念事項にまで高まってきたことで、細かな規制が増大しています。このような規制は、製品とサービスそのものにとどまらず、製品とサービスを提供する企業をも対象としています。フィリップスは、自社のサプライチェーンに対する責任のみならず、お客様のサプライチェーンの一部としての当社の役割と責任を認識しています。

「情報セキュリティは、品質と同様に、当社のDNAに組み込まれ、当社のあらゆる事業活動に統合される必要があります。」

Wim Sonnemans
Head of Information Security, Royal Philips

製造販売業者
株式会社フィリップス・ジャパン
〒106-0041　東京都港区麻布台1-3-1
麻布台ヒルズ森JPタワー15階
お客様窓口　0120-556-494
03-4334-7637
受付時間　9:00～18:00（土・日・祝祭日・年末年始を除く）

www.philips.co.jp/healthcare

2586077
0925PDF01-TP　Printed in Japan